Kriptografi dalaam Industri Game Indonesia

Adrian Edbert Luman - 13507057
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

***Abstrak* – Makalah ini membahas mengenai penerapan kriptografi dalam industri game. Industri game merupakan sebuah industri yang sedang berkembang di Indonesia. Industri game menggunakan kriptografi untuk banyak sekali hal. Misalnya dalam copy protection, yaitu cara mencegah pembajakan sebuah game, ataupun yang sederhana seperti mengenkripsi file dalam game agar tidak mudah dibajak dan menimbulkan cheat yang tidak diinginkan. Makalah ini akan membahas mengenai penggunaan kriptografi tersebut dan masalah terkait kriptografi yang telah terjadi maupun sedang terjadi. Makalah ini juga akan mencoba untuk memberikan solusi terhadap masalah kriptografi dalam industri game.**

Kata Kunci : industri game, copy protection, cheat, game data, saved data

I. PENDAHULUAN

Industri game merupakan sebuah industri yang telah lama ada, namun di Indonesia sendiri industri game bisa dibilang merupakan industri yang masih berkembang. Dengan semakin banyak dan canggihnya teknologi untuk meng-hack sebuah video game, maka pengetahuan mengenai kriptografi sangat diperlukan oleh industri game di Indonesia. Pengetahuan mengenai kriptografi dalam industri game Indonesia, terutama yang telah dilakukan oleh perusahaan luar, dapat menjaga keamanan HAKI para developer game di Indonesia.

Di luar Indonesia, penggunaan kriptografi untuk melindungi keamanan sebuah game sudah ada sejak pertama kali game itu sendiri ada. Namun cara yang digunakan masih tergolong kriptografi primitif, sebab kriptografi tidak diterapkan ke dalam data atau media penyimpanan dari game itu sendiri. Dalam dunia modern kriptografi dalam video game telah berkembang lebih jauh, namun penggunaannya dalam copy protection masih bisa dibilang primitif, sebab kriptografi lebih diterapkan ke bagaimana cara hardware sebuah game membaca media penyimpanan. Analisis terhadap penggunaan kriptografi dalam game data untuk melindungi copy protection di Indonesia akan coba dilakukan dalam makalah ini.

Selain digunakan untuk copy protection, kriptografi juga ditemukan untuk melindungi data dalam game. Data game yang dienkripsi biasanya adalah data permainan yang disimpan, hal ini dikarenakan data permainan, atau saved data, merupakan kumpulan informasi mengenai apa yang sudah dilakukan oleh pemain. Saved data yang tidak dienkripsi akan sangat mudah untuk diretas dan menyebabkan hal-hal yang tidak dimaksudkan dalam game terjadi, seperti misalnya cheat atau crash. Dalam makalah ini akan coba diimplementasikan penggunaan kode hash untuk melindungi isi dari saved data.

Kriptografi dalam industri game ikut berkembang bersama dengan industri game itu sendiri. Sejak industri game mulai beralih ke dunia online timbul banyak masalah baru, keamanan data pengguna. Tanpa metode kriptografi yang baik, keamanan data pengguna terancam digunakan oleh pihak ketiga untuk tujuan yang tidak benar. Dalam kasus ini makalah akan membahas mengenai peretasan server dari Play Station Network dampak serta perencanaan solusi.

II. LANDASAN TEORI

A. Copy Protection

1. Copy protection spesifik untuk game lama

   Pada tahun 1980 dan 1990-an, game komputer yang dijual melalui *audio castte* dan *floppy disk* dilindungi menggunakan sebuah metode yang interaktif terhadap pengguna yang mengharuskan pengguna memiliki paket penyimpanan asli, biasanya dalam bentuk manual. Copy protection tidak diaktifasi setiap instalasi namun setiap game dijalankan.

   Terkadang kode copy protection tidak dijalankan pada saat awal, namun pada pertengahan game. Seperti misalnya pada game Konami berjudul Metal Gear Solid untuk Sony PlayStation One, di mana pemain harus melihat belakang kotak cd mereka untuk mendapat frekuensi radio tertentu dan melanjutkan permainan.

Salah satu metode copy protection lama yang paling menarik adalah dalam game The Secret of Monkey Island buatan Lucasfilm Games di mana dalam manual disertakan sebuah lingkaran berisi wajah, dalam game nantinya pemain akan menemukan puzzle yang mengharuskan penggunaan lingkaran tersebut.

2. Copy protection modern

   Konsol game jaman sekarang menerapkan copy protection dalam level hardware. Microsoft Xbox misalnya, konsol perusahaan Bill Gates ini menggunakan metode non-booting atau non-reading dari CD dan DVD-R, dalam Xbox terdapat metode pembacaan record dari luar ke dalam sehingga disc Xbox seolah berputar terbalik ketika pembuatan.

   Sony PlayStation 3 menggunakan BD-ROM yang dilindungi oleh ROM-Mark yang tidak dapat diduplikasi oleh alat perekam yang dimiliki user. Pada ROM-Mark terdapatVolume ID yang digunakan untuk dekripsi konten BD-ROM menggunakan AACS.

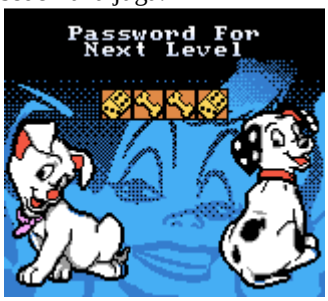
B. Saved Data

Saved data adalah sebuah data kecil informasi yang disimpan sebagai progress seorang pemain dalam game.

Pada awal era game, saved data tidak diperlukan. Hal ini dikarenakan game yang ada pada waktu itu tidak memiliki cerita dan rentang waktu permainannya sebentar. Seperti misalnya permainan tetris. Seiring berkembangnya game kebutuhan untuk saved data meningkat.

1. Password

   Ketika hardware belum mendukung penyimpanan data, dan penyimpanan data dalam media eksternal terlalu mahal untuk saat itu. Penggunaan password sebagai saved data merupakan solusi utama. Password bisa merupakan sekumpulan kode untuk loncat ke bagian tertentu dari game atau memberikan kesempatan kepada pemain untuk melakukan cheat secara legal. Kompleksitas password biasanya tergantung dari game itu sendiri, game dengan sistem yang kompleks membutuhkan password dengan kompleksitas tinggi juga, sementar game dengan kompleksitas sederhana dapat menggunakan password yang sederhana juga.

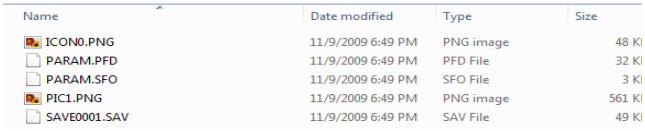


2. Saved Data

   Saved data digunakan untuk menggantikan password sejak hardware telah berevolusi, tersedianya media penyimpanan eksternal untuk konsol game memberikan kemudahan untuk menyimpan sebuah saved game. Saved data menjadi semakin penting sejak game menjadi semakin kompleks dan menggunakan password menjadi terlalu kompleks untuk pemain.

   Saved data pada Sony PlayStation 3 misalnya menggunakan metode enkripsi yang berbeda-beda tergantung dari developernya.

   Dalam Sony PlayStation 3, format saved data umunya terdiri dari 3 bagian, yaitu file png untuk icon pada saved data, file PFD yang merupakan inti dari kriptografi saved data, file SFO yang merupakan system file dari Sony, serta file savedata itu sendiri yang berbeda-beda untuk setiap game.



Name	Date modified	Type	Size
ICON0.PNG	11/9/2009 6:49 PM	PNG image	48 KI
PARAM.PFD	11/9/2009 6:49 PM	PFD File	32 KI
PARAM.SFO	11/9/2009 6:49 PM	SFO File	3 KI
PIC1.PNG	11/9/2009 6:49 PM	PNG image	561 KI
SAVE0001.SAV	11/9/2009 6:49 PM	SAV File	49 KI

C. Online Encryption

Perkembangan dunia game mengubah kriptografi dalam video game. Kalau dalam era sebelum online kriptografi digunakan karena hubungan antara orang dengan konsol game miliknya. Sekarang kriptografi digunakan sebagai hubungan antara orang dengan dunia.

Salah satu penggunaan kriptografi pada era online adalah sistem hash pada record best lap untuk permainan Initial D. Hash digunakan agar user tidak bisa mengarang best lap mereka sendiri yang tentunya akan mengurangi kredibilitas ranking best lap pada situs resmi Initial D.

Penggunaan lain adalah enkripsi user data pada server. Tanpa enkripsi akan sangat berbahaya ketika server berhasil diretas oleh pihak ketiga, karena semua data konfidensial user dapat langsung digunakan oleh pihak ketiga.

III. KRIPTOGRAFI GAME DI INDONESIA

A. Copy Protection di Indonesia

Indonesia merupakan negara berkembang dalam bidang industri video game, oleh karena itu penggunaan copy protection masih tergolong bergantung pada negara lain. Seperti misalnya metode copy protection pada game buatan lokal yang di-publish di application store Android bergantung pada metode copy protection dari Android itu sendiri. Melihat dari metode-metode copy protection yang sudah ada sebelumnya Indonesia sendiri akan kesulitan untuk menggunakan metode-metode copy protection tersebut. Oleh karena itu maka metode copy protection yang baru diperlukan.

Beberapa solusi yang mungkin:

1. Proteksi file executable dan resource

   Proteksi file exe memungkinkan salah satunya dengan menggunakan applikasi yang disebut dengan MoleBox.

MoleBox dapat membuat applikasi game yang sudah dibuat agar:
-File executable tidak berada dalam paket, hal ini agar dapat diaplikasikan wrappers dan mengurangi resiko false alarm dari anti-virus.
-Membuat paket data tetap eksternal atau disatukan dengan file exe, sehingga tercipta sebuah file executable untuk keseluruhan aplikasi.
-Mendapat kemampuan untuk mengatur waktu dan urutan dari aplikasi, maksudnya adalah developer mampu memberi batas waktu exipred pada applikasi sekaligus juga memberi password atau serial number.

Di Indonesia di mana mayoritas applikasi didapat dengan cara diunduh melalui internet cara ini dapat diaplikasikan dengan baik, karena tanpa kunci dari developer meskipun pengguna dapat mengunduh aplikasi namun aplikasi tidak dapat berjalan.

Sayangnya kelemahan dari sistem ini jelas mengenai shared-key, dengan MoleBox di mana kita memberikan sebuah password kepada pengguna yang membeli, apabila pengguna yang membeli memberikan kunci itu kepada orang lain, maka kredibilitas kunci tidak dapat dipertahankan sebab kunci pada aplikasi tidak dapat dijamin keunikannya, yang berarti kunci yang sama dapat digunakan untuk membuka aplikasi pada banyak komputer berbeda.

2. Sistem Dongle

   Atau bisa disebut sebagai hardware key, sebuah sistem dimana tanpa dongle yang biasanya berbentuk USB-Drive applikasi tidak dapat dijalankan.

Penggunaan dongle untuk copy protection game terutama di Indonesia akan terasa aneh bila diimplementasikan di Indonesia, sebab di luar Indonesia sekalipun dongle bukan merupakan sebuah hal yang umum. Hal ini karena biaya produksi yang akan meningkat karena adanya dongle yang harus dijual bersama dengan aplikasi. Dongle ini sendiri tidak 100% kredibilitas sebab satu dongle dapat digunakan lebih di satu komputer, namun lebih baik daripada penggunaan password, sebab tidak memungkinkan lebih dari satu aplikasi berjalan paralel bila hanya terdapat satu buah dongle.

B. Saved Data di Indonesia

Penerapan pengamanan metode saved data yang pernah ada dapat diterapkan di Indonesia. Salah satu metode yang efektif adalah penggunaan kode hash dalam saved data.

Misalkan dalam saved data sebuah game disimpan nilai-nilai yang merepresentasikan waktu permainan dan nilai-nilai lain. Apabila tidak dienkripsikan makan file saved data tersebut bisa saja diubah-ubah dengan menggunakan editor sederhana menyebabkan game menjadi tidak menarik atau crash. Penggunaan nilai hash dalam file saved data menyebabkan file dapat diperiksa kebenarannya menggunakan fungsi hash tersebut agar tidak terjadi hal tersebut. Fungsi hash digunakan karena termasuk kuat dalam keunikannya dan nilai yang dihasilkan tidak panjang, sehingga tidak mengubah ukuran file saved data secara eksponensial.

Di Indonesia sendiri pengamanan saved data masih belum di rasa penting dibandingkan dengan copy protection, hal ini dikarenakan kalau copy protection lemah akan memberikan dampak secara langsung kepada developer, namun penanganan saved data hanya akan berdampak pada user, dan tidak dalam skala besar. Resiko terbesar yang dihadapi user hanyalah file saved data yang corrupt atau kesenangan bermain yang hilang. Namun apabila ditangani secara asal-asalan nantinya ketika game buatan industri lokal semakin meningkat secara kompleksitas, dan tidak memperbolehkan adanya kesalahan dalam penanganan saved data, penanganan sejak awal seiring berkembangnya industri merupakan usaha untuk menangani masalah yang akan ditemui nantinya.

C. Online Protection di Indonesia

Penerapan sistem online protection sendiri masih samar, sebab perusahaan besar tidak akan membocorkan rahasia perusahaan dalam penyimpanan data user, hal itu akan menurunkan tingkat kepercayaan user pada perusahaan.

Di Indonesia di mana game online saat ini merupakan pasar terbesar game, pengamanan data user merupakan hal yang sangat penting. Salah satu informasi user yang paling penting dan tidak boleh sampai hilang adalah nomor kartu kredit. Di luar Indonesia, penggunaan kartu kredit sebagai alat bayar utama transaksi online merupakan hal yang umum, namun di Indonesia hal ini masih jarang sehingga umumnya pendaftaran online tidak meminta nomor kartu kredit. Apakah hal ini berarti tidak ada data penting yang disimpan di server-server game online yang ada di Indonesia. Sebagai seorang pengguna, data permainan yang disimpan itu sendiri merupakan hal berharga yang bisa bernilai sejumlah uang. Ya, di Indonesia penjualan e-objects di game menjadi uang nyata dalam rupiah sudah menjadi hal yang umum. Oleh karena itu apabila data tersebut diretas dan hilang atau dimodifikasi bisa berarti kerugian langsung kepada user, bahkan nilainya bisa sampai ratusan juta untuk game tertentu.

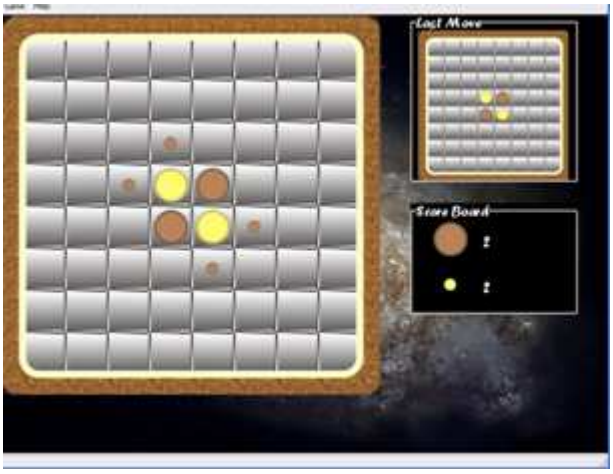
Masalah yang baru saja terjadi pada Sony PlayStation Network (PSN) merupakan hal yang bisa menjadi pelajaran bagi Indonesia. 77 juta informasi user diretas oleh hacker yang menyebut diri “mereka” sebagai ‘Anonymous’. Menurut Sony data paling konfidensial dari user data yang ada yaitu data mengenai kratu kredit terenkripsi, namun tidak menutup kemungkinan informasi tersebut berhasil dienkripsi oleh hacker, seperti dikutip oleh Sony dalam blognya: “While all credit card information stored in our systems is encrypted and there is no evidence at this time that credit card data was taken, we cannot rule out the possibility.”

Hingga makalah ini ditulis Sony masih belum dapat menangkap ‘Anonymous’ dan PSN masih belum dapat diakses sampai sekarang.

V. PENGUJIAN

Yang akan diuji di sini adalah pengujian penggunaan hash untuk file saved data. Game yang akan digunakan untuk pengujian adalah game Donthello yang merupakan sebuah game reversi. Donthello sendiri merupakan tugas

Strategi Algoritma yang dimodifikasi agar dapat menyimpan permainan dan membuka kembali file saved data. Donthello dibuat oleh penulis bersama rekan mahasiswa Filman Ferdian dan Kamal Mahmudi.



Dalam game ini file saved data memiliki format seperti di bawah ini:

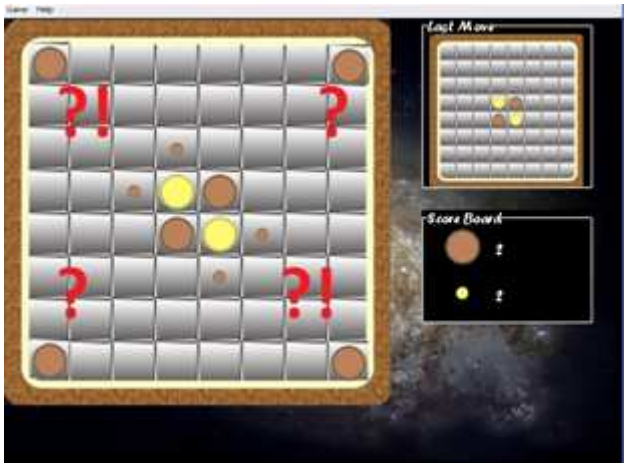
```
2-2
Black
00000000
00000000
00000000
000WB000
000BW000
00000000
00000000
00000000
```

Baris pertama menunjukkan skor kedua pemain, baris kedua menunjukkan giliran jalan pemain, dan 8 baris berikutnya merepresentasikan board. Save data tersebut merepresentasikan kondisi awal permainan.

Tanpa adanya penanganan saved data maka file tersebut bisa diubah merusak peraturan reversi yang ada, misalnya:

```
2-2
Black
B000000B
00000000
00000000
000WB000
000BW000
00000000
00000000
B000000B
```

Yang mengubah layar permainan menjadi:



Hal ini membuat permainan tidak menarik dan memberikan keuntungan yang tidak adil untuk pemain hitam.

Oleh karena itu penggunaan kode hash haruslah ada agar tidak mungkin terjadi pengeditan file saved data seperti di atas.

Contoh saved data setelah disisipkan hash:

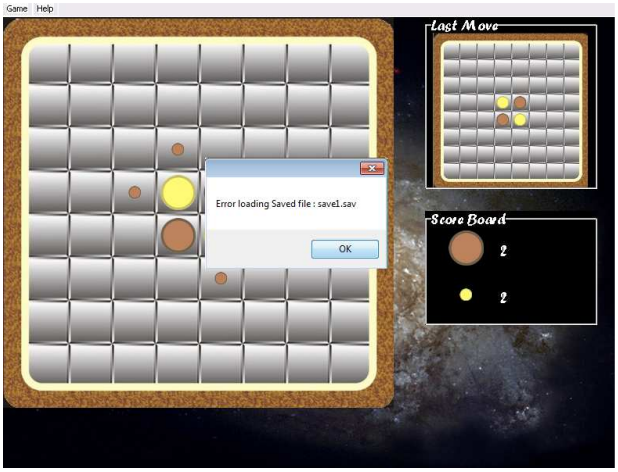
```
2-2
Black
00000000
00000000
00000000
000WB000
000BW000
00000000
00000000
00000000
7B9AB294EFD4E7DCEBD5185E0839E1F2B387BDD4
```

Baris terakhir adalah nilai hash-nya.

Bila sebuah file tidak cocok dengan hash yang disisipkan maka akan menimbulkan pesan error, misalnya dengan file yang sama:

```
2-2
Black
B000000B
00000000
00000000
000WB000
000BW000
00000000
00000000
B000000B
7B9AB294EFD4E7DCEBD5185E0839E1F2B387BDD4
```

Akan menghasilkan:



Sistem pengecekan error ini mirip dengan digital signature di mana file save data akan dimasukkan ke fungsi hash kemudian dicocokkan dengan nilai hash yang ada pada saved data itu sendiri.

VI. KESIMPULAN DAN SARAN

Copy Protection di Indonesia masih dirasa merupakan suatu hal yang ambigu dan sangat sulit. Sebab kesadaran masyarakat Indonesia akan HAKI sangatlah rendah. Oleh sebab itu developer game harus pintar terutama dalam pemasyarakatan HAKI itu sendiri, sebab tidak ada sistem keamanan yang tidak dapat ditembus, satu-satunya hal yang bisa membuat game yang 100% tidak dapat dibajak adalah kesadaran dari manusia itu sendiri.

Pengamanan saved data menggunakan kode hash dirasa sudah cukup untuk menangani kasus edit saved data. Selama hacker tidak dapat menggunakan fungsi hash yang sama untuk menghasilkan file hash yang sesuai dengan editan saved data yang dia buat.

Metode pengamanan saved data lebih lanjut dapat menggunakan digital signature yang menggabungkan fungsi RSA dan hash agar menghasilkan sistem yang lebih aman.

Online protection di Indonesia sampai saat ini dibilang cukup aman, meskipun banyaknya cheat yang ada pada game-game online yang ada di Indonesia, namun belum sampai ada yang meretas server-server game online yang ada di Indonesia, atau setidaknya belum sampai menimbulkan kerugian berskala besar, seperti dialami Sony dengan PSN-nya.

Lebih jauh lagi perusahaan game online hendaknya mempekerjakan ekspert di bidang sekuriti agar tidak terjadi hal-hal yang tidak diinginkan. Hal ini akan sangat berguna untuk menjaga kepercayaan dari user, dan kerugian uang yang besar.

DAFTAR PUSTAKA

R. Munir, “Diktat Kuliah IF5054 Kriptografi”, Program Studi Teknik Informatika, Institut Teknologi Bandung, 2006.
http://en.wikipedia.org/wiki/Copy_protection
http://en.wikipedia.org/wiki/ROM-Mark
http://en.wikipedia.org/wiki/Advanced_Access_Content_System
http://ps3dev.wikispaces.com/
http://en.wikipedia.org/wiki/Software_protection_dongle
http://www.molebox.com/
http://www.info-mech.com/drm_cryptography.html
http://ps3.ign.com/articles/115/1159426p1.html
http://blog.us.playstation.com/2011/04/27/qa-1-for-playstation-network-and-qriocity-services/
http://www.anonnews.org/?p=press&a=item&i=797
http://www.ps3savegame.com/

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 09 Mei 2011

ttd

Adrian Edbert Luman dan 13507057